IN THE CLAIMS:

We claim:

1. (Withdrawn) A system comprising:

client computers having one or more data records, the client computers in communication with a network, the client computers configured to field-level normalize and encrypt one or more fields of the one or more data records to provide one or more de-identified records; and

a server computer in communication with the network to receive the one or more de-identified records and in communication with a database, the database including one or more master records, the server computer configured to compare the one or more de-identified records with the one or more master records and to determine which records of the one or more de-identified records and the one or more master records are to be linked.

2. (Withdrawn) The system of claim 1 wherein the database is partially described by a table of master records.

3. (Withdrawn) The system of claim 2 wherein the table is for comparing the one or more de-identified records are compared with the one or more master records.

4. (Withdrawn) A method for de-identification of at least one record by a programmed client computer, comprising:

obtaining the at least one record, the at least one record having data fields;

normalizing at least a portion of the data fields; and

first encrypting the at least a portion of the data fields to provide a de-identified record.

5. (Withdrawn) The method of claim 4 further comprising: second encrypting the de-identified record;

compressing the de-identified record; and

transmitting the de-identified record.

6. (Withdrawn) The method of claim 5 further comprising encoding the data fields after normalization.

7. (Withdrawn) A method for de-identification of records by and at a programmed client computer, comprising:

providing records to the programmed client computer;

locating personal identification data fields in each of the records;

parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected; and encrypting the personal identification data fields selected.

8. (Withdrawn) The method of claim 7 further comprising:

obtaining a mapping file; and

locating personal identification data fields in each of the records using the mapping file.

9. (Withdrawn) The method of claim 7 further comprising:

determining if the personal identification data fields selected are to be encoded; and

encoding the personal identification data fields to be encoded.

10. (Withdrawn) The method of claim 9 further comprising concatenating the personal identification data fields encoded with a seed value to provide seed value identifiers.

11. (Withdrawn) The method of claim 9 wherein the personal identification data fields are not concatenated with a seed value prior to the encrypting.

12. (Withdrawn) The method of claim 7 wherein the encrypting step comprises:

one-way encrypting with a first encryption algorithm the personal identification data fields selected to provide a first encryption result for each of the personal identification data fields selected; and

one-way encrypting with a second encryption algorithm the personal identification data fields selected to provide a second encryption result for each of the personal identification data fields selected.

13. (Withdrawn) The method of claim 12 wherein the encrypting step comprises:

concatenating at least a portion of each of the first encryption result and the second encryption result for each of the personal identification data fields to respectively provide binary string identifiers for the personal identification data fields; and

converting the binary strings to alphanumeric strings to provide match codes.

14. (Withdrawn) A method for de-identification of records by a programmed client computer, comprising:

monitoring a file directory;

detecting presence of a new file in the file directory;

obtaining a mapping file for the new file;

locating personal identification data fields in records in the new file

using the mapping file; parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected;

determining if the personal identification data fields selected are to be encoded;

encoding the personal identification data fields to be encoded;

concatenating the personal identification data fields encoded with a

seed value to provide seed value identifiers;

first encrypting the seed value identifiers with a first encryption algorithm; second encrypting the seed value identifiers with a second encryption algorithm;

concatenating at least a portion of each encryption result from the first encrypting and the second encrypting corresponding to the seed value identifiers to respectively provide binary strings for each of the seed value identifiers; and

converting the binary strings to alphanumeric strings to provide match codes;

wherein de-identified records comprising the match codes are created at the programmed client computer prior to transmission to a server computer.

15. (Withdrawn) A signal-bearing medium containing a program which, when executed by a processor, causes execution of a method comprising:

obtaining at least one record, the record having data fields;

normalizing at least a portion of the data fields; and

encrypting the at least a portion of the data fields to provide a de-identification record.

16. (Withdrawn) A signal-bearing medium containing a program which, when executed by a programmed client computer, causes execution of a method comprising:

providing records to the programmed client computer;

locating personal identification data fields in each of the records;

parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected; and

encrypting the personal identification data fields selected.

17. (Withdrawn) A signal-bearing medium containing a program which, when executed by a programmed client computer, causes execution of a method comprising:

monitoring a file directory;

detecting presence of a new file in the file directory;

obtaining a mapping file for the new file;

locating personal identification data fields in records in the new file using the mapping file;

parsing the personal identification data fields;

formatting the personal identification data fields;

selecting at least a portion of the personal identification data fields formatted;

deleting any of the personal identification data fields not selected;

determining if the personal identification data fields selected are to be encoded;

encoding the personal identification data fields to be encoded;

concatenating the personal identification data fields encoded with a seed value to provide seed value identifiers;

first encrypting the seed value identifiers with a first encryption algorithm;

second encrypting the seed value identifiers with a second encryption algorithm;

concatenating at least a portion of each encryption result from the first encrypting and the second encrypting corresponding to the seed value identifiers to respectively provide binary strings for each of the seed value identifiers; and

converting the binary strings to alphanumeric strings to provide match codes;

wherein de-identified records comprising the match codes are created at the programmed client computer prior to transmission to a server computer.

18. (Original) A method for linkage of de-identified records, comprising:

obtaining client de-identified records, the client de-identified records comprising field-level encrypted match codes;

providing a database of master de-identified records, the master de- identified records comprising field-level encrypted match codes;

comparing the match codes of the client de-identified records and the master de-identified records; and

linking at least a portion of the client de-identified records with the master de-identified records using comparison of the match codes.

19. (Original) The method of claim 18 further comprising assigning identification codes to the master de-identified records.

20. (Original) The method of claim 19 further comprising appending the identification codes of the master de-identified records to the client de-identified records.

21. (Withdrawn) A method for transforming personal identifying information to facilitate protection of privacy interests while allowing use of non-personally identifying information, comprising:

receiving data on an individual including personally identifying information,

de-identifying the data at a client computer including field-level encryption,

transmitting the de-identified data to a server computer for record linkage, and

using match codes created for the data at the client computer to link records at the server computer.

22. (Withdrawn) The method of claim 21 wherein the field-level encryption is one-way encryption.

23. (Withdrawn) The method of claim 21 wherein the field-level encryption is two-way encryption.

24. (Withdrawn) A method for re-identification of de-identified files, comprising:

providing a client computer; creating original information records at the client computer;

de-identifying at least a portion of the original information records at the client computer to provide match codes;

maintaining the match codes of the de-identified records in association with the original information records in a database associated with the client computer;

providing a server computer;

transmitting the match codes of the de-identified records to the server computer;

longitudinally linking the de-identified records using the match codes at the server computer;

providing the de-identified records longitudinally linked to the client computer;

comparing using the match codes the de-identified records longitudinally linked to the de-identified records maintained to reidentify the de-identified records longitudinally linked.

25. (Withdrawn) The method of claim 24 wherein the original information records comprise consent indicators.

26. (New) A system that links de-identified records, comprising:

a server computer that obtains client de-identified records, wherein the client de-identified records comprise first field-level encrypted match codes; and

a database that stores a plurality of master de-identified records, wherein the master de-identified records comprise second field-level encrypted match codes,

wherein the server computer is adapted to compare the first field-level encrypted match codes and the second field-level encrypted match codes and link at least a portion of the client de-identified records with the master de-identified records based on a comparison of the first field-level encrypted match codes and the second field-level encrypted match codes.

27. (New) The system of claim 26 wherein the server computer is further adapted to probabilistically link said at least a portion of the client de-identified records with the master de-identified records.

28. (New) The system of claim 26 further comprising a table used to facilitate a link of said

at least a portion of the client de-identified records with the master de-identified records.

29. (New) The system of claim 26 wherein the server computer comprises a communication interface used to receive the client de-identified records from one or more client computers.

30. (New) A system that links de-identified records, comprising:

a database that stores a plurality of master de-identified records; and

a server communicatively coupled to the database to link at least a portion of client de-identified records with the master de-identified records based on a comparison of match codes.

31. (New) The system of claim 30 further comprising a table used to facilitate a link of said at least a portion of the client de-identified records with the master de-identified records.

32. (New) The system of claim 30 wherein the match codes are encrypted.

33. (New) The system of claim 30 wherein the server comprises an interface to receive the client de-identified records from a plurality of client computers.

34. (New) The system of claim 30 wherein the server is adapted to compare match codes of the master de-identified records with match codes of the client de-identified records.

35. (New) The system of claim 30 wherein the master de-identified records comprise assigned identification codes.

36. (New) The system of claim 35 wherein the server is further configured to append the assigned identification codes to the client de-identified records.

37. (New) A system that links de-identified records, comprising:

means for obtaining client de-identified records, the client de-identified records comprising field-level encrypted match codes;

means for providing a database of master de-identified records, the master de- identified records comprising field-level encrypted match codes;

means for comparing the match codes of the client de-identified records and the master de-identified records; and

means for linking at least a portion of the client de-identified records with the master de-identified records using comparison of the match codes.

38. (New) The system of claim 37 further comprising means for assigning identification codes to the master de-identified records.

39. (New) The system of claim 37 further comprising means for appending the identification codes of the master de-identified records to the client de-identified records.

40. (New) The system of claim 37 wherein at least one of the client de-identified records has a personal identification data field that is encoded with a seed value to provide seed value identifiers.

41. (New) A method for linkage of de-identified records, comprising:

receiving client de-identified records;

comparing match codes of the client de-identified records with match codes of master de-identified records; and

linking at least a portion of the client de-identified records with the master de-identified records in response to comparing the match codes of the client de-identified records with match codes of master de-identified records.

42. (New) The method of claim 41 further comprising assigning identification codes to the master de-identified records.

43. (New) The method of claim 42 further comprising appending the identification codes of the master de-identified records to the client de-identified records.

44. (New) The method of claim 41 wherein the match codes of the client de-identified records are encrypted.

45. (New) The method of claim 41 wherein linking at least a portion of the client de-identified records with the master de-identified records comprises probabilistically linking said at least a portion of the client de-identified records with the master de-identified records.

46. (New) The method of claim 41 further comprising appending identification codes of the master de-identified records to the client de-identified records.